UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: GWENDOLYN SMUDA and STEVEN CHECCHIA, *on behalf of themselves and all others similarly situated*, Plaintiffs, v. TEACHERS INSURANCE AND ANNUITY ASSOCIATION OF AMERICA, PENSION BENEFIT INFORMATION, LLC, and PROGRESS SOFTWARE CORPORATION, Defendants.	MDL No. 1:23-md-03083-ADB-PGL **AMENDED CLASS ACTION COMPLAINT** CIVIL ACTION NO. 1:23-cv-12773

Plaintiffs, Gwendolyn Smuda ("Plaintiff Smuda") and Steven Checchia ("Plaintiff Checchia") (together, "Plaintiffs"), bring this Class Action Complaint ("Complaint") against Teachers Insurance and Annuity Association of America ("TIAA"), Pension Benefit Information, LLC ("PBI"), and Progress Software Corporation ("PSC") (together with TIAA and PBI, "Defendants"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs incorporate the allegations contained in Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

2. Plaintiffs seek monetary damages and injunctive and declaratory relief in this

action, arising from Defendants' failure to safeguard the Personally Identifiable Information[1] ("Private Information" or ("PII")) of their customers, which resulted in unauthorized access to their information systems on May 29 and May 30, 2023, and the compromised and unauthorized disclosure of that Private Information, causing widespread injury and damages to Plaintiffs and the proposed Classes (defined below).

3. TIAA is a New York, New York-based Fortune 100 financial services organization that is a provider of financial services in the academic, research, medical, cultural, and governmental fields. It serves over 5 million active and retired employees participating at more than 15,000 institutions and has $1 trillion in combined assets under management with holdings in more than 50 countries (as of December 31, 2017).[2]

4. As explained in detail herein, an unauthorized third party accessed Defendants' MOVEit Transfer servers and accessed and removed PII from the servers as early as May 27, 2023[3] (the "Data Breach").

5. As a result of the Data Breach, which Defendants failed to prevent, the Private Information of Defendants' customers, including Plaintiffs and the proposed Class members, were stolen. The exposed information includes the following: name, Social Security number, date of birth, address, and gender.

---

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendants, not every type of information included in that definition was compromised in the subject data breach.

[2] https://en.wikipedia.org/wiki/Teachers_Insurance_and_Annuity_Association_of_America (last visited Aug. 6, 2023).

[3] https://www.reuters.com/technology/hackers-use-flaw-popular-file-transfer-tool-steal-data-researchers-say-2023-06-02/; https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html.

6. Defendants' investigation concluded that the Private Information compromised in the Data Breach included Plaintiffs' and over 2.5 million other TIAA customers' information (together, "Customers").[4]

7. Defendants' failure to safeguard Customers' highly sensitive Private Information as exposed and unauthorizedly disclosed in the Data Breach violates their common law duty, state laws, and Defendants' implied contract with the Customers to safeguard their Private Information.

8. Plaintiffs and Class members now face a lifetime risk of identity theft due to the nature of the information lost, including Social Security numbers, which they cannot change, and which cannot be made private again.

9. Defendants' harmful conduct has injured Plaintiffs and Class members in multiple ways, including: (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

10. Defendants' failure to protect Plaintiffs' and the Classes' Private Information has harmed and will continue to harm Plaintiffs and the Classes, causing Plaintiffs to seek relief on a class wide basis.

11. On behalf of themselves and the Classes preliminarily defined below, Plaintiffs bring causes of action against Defendants for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and declaratory judgment, seeking an award of monetary damages and injunctive and declaratory relief, resulting from Defendants' failure to adequately protect their

[4] https://www.databreaches.net/teachers-insurance-and-annuity-association-of-america-notifying-2630717-after-pbi-alerts-them-to-moveit-breach/ (last visited Aug. 7, 2023).

highly sensitive Private Information.

PARTIES

Plaintiff Smuda

12. Plaintiff Smuda is, and at all times material hereto was, an individual resident and citizen of the state of Illinois.

13. Plaintiff Smuda provided Private Information to Defendants on the condition that it be maintained as confidential and with the understanding that Defendants would employ reasonable safeguards to protect her Private Information.

14. If Plaintiff Smuda had known that Defendants would not adequately protect her Private Information, she would not have allowed Defendants to maintain this sensitive Private Information.

Plaintiff Checchia

15. Plaintiff Checchia is, and at all times material hereto was, an individual resident and citizen of the state of Pennsylvania.

16. Plaintiff Checchia provided Private Information to Defendants on the condition that it be maintained as confidential and with the understanding that Defendants would employ reasonable safeguards to protect his Private Information.

17. If Plaintiff Checchia had known that Defendants would not adequately protect his Private Information, he would not have allowed Defendants to maintain this sensitive Private Information.

Defendants

18. TIAA is a not for profit corporation organized under the laws of New York with its headquarters and principal place of business at 730 Third Avenue, New York, New York 10017.

19. TIAA is a Vendor Contracting Entity of PBI. *See* Plaintiffs' Omnibus Set of

Additional Pleading Facts, Appendix A.

20. PBI is a for-profit Delaware corporation with its principal place of business at 333 S 7th Street, Suite 2400, Minneapolis, MN 55402. PBI uses PSC's MOVEit service in the regular course of its business acting as a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans.[5]

21. PBI is a PSC Vendor. *See* Plaintiffs' Omnibus Set of Additional Pleading Facts, Appendix A.

22. PSC is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803. PSC offers the service MOVEit, which experienced the Data Breach underlying Plaintiffs' claims.

JURISDICTION AND VENUE

23. This case was originally filed in the United States District Court for the Southern District of New York. This action was transferred to this Court for coordinated or consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407 and Rule 7.1 of the Rules of Procedure of the United States Judicial Panel on Multidistrict Litigation.

24. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed classes, and at least one member of the classes is a citizen of a state different from Defendants.

25. The United States District Court for the Southern District of New York has personal jurisdiction over Defendants because TIAA's principal place of business is in that District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from that District.

[5] https://www.pbinfo.com/ (last visited August 1, 2023).

Defendants have sufficient contacts in New York, as they conduct a significant amount of business in the state of New York.

26. Venue is proper in the Southern District of New York under 18 U.S.C. § 1391(a) through (d) because a substantial part of the events or omissions giving rise to the Plaintiffs' claims occurred in that District.

FACTUAL BACKGROUND

Defendants' Businesses

27. TIAA is a New York, New York-headquartered financial services company.

28. PBI provides audit and address research services for insurance companies, pension funds, and other organizations, including TIAA.

29. PBI is a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans, and one of the many companies that uses PSC's MOVEit service to transfer large amounts of data in the ordinary course of its business and the service it provides to pension plans and other organizations.[6]

30. According to the Notice Letter received by Plaintiff, PBI provides audit and address research services for Corebridge.

31. PBI's website also promises consumers that it has robust systems and processes in place to protect and secure their sensitive information:

[6] https://www.pbinfo.com/ (last visited August 1, 2023).

Protecting and securing the information of our clients and our company is of critical importance to PBI. We recognize that all relationships with current and prospective clients are based upon integrity and trust, and we take our role as custodians of confidential information very seriously.

PBI uses a multi-layered approach to protect data securely that includes, but is not limited to the following: implementing secure development practices, including annual training for our IT team, real time scanning of code changes for vulnerabilities, web application firewalls, n-tier application architecture, required security awareness training program for all employees at onboarding and on a regular basis, data loss prevention tools to alert and block transfers of sensitive data, and a consolidated SIEM solution that correlates alerts and events across multiple environments. PBI's data security team manages this multi-layered security architecture by performing over 30 security reviews of quarterly audit checks to test compliance against security policies.

PBI's formalized security program follows the industry-recognized security policy frameworks from the National Institute of Science & Technology (NIST) SP 800-53 and NIST Cybersecurity Framework.

SOC2 Audit and Third-party Security Testing

PBI undergoes an annual SSAE 18 SOC 2, Type II audit by an independent third-party to audit our controls over data confidentiality, integrity, security, and availability.

PBI regularly uses third parties to test and audit our security controls. We conduct monthly and quarterly vulnerability assessments and penetration tests of PBI's internal and external network and application security, and conduct annual application penetration tests.

32. PBI's website also tells consumers that it has systems and process in place to ensure

the privacy of their sensitive information obtained over the internet and to prevent identity theft:

> **9. ONLINE PRIVACY**
>
> PBI strives to protect the privacy of personally identifiable information obtained over the Internet and strives to apply the Principles and evolving standards to the online environment.
>
> **10. IDENTITY THEFT**
>
> PBI strives to prevent the acquisition of information from our products and services for improper purposes, such as identity theft. PBI believes in the importance of notifying individuals who may have had their sensitive personally identifiable information acquired by an unauthorized individual, as appropriate.

33. Furthermore, PBI acknowledges that it has a duty to safeguard Plaintiffs' and Class Members' sensitive PII because, inter alia, PBI's website tells consumers that it has systems in place to protect consumers' sensitive information, and routinely audits those systems to ensure they are compliant with federal regulations and other legislation—as well as industry standards and practices— governing data privacy:

> **8. ACCOUNTABILITY**
>
> PBI supports accountability of information industry standards and practices, responsible and effective federal regulation of the data industry, and legislation governing the practices of all data providers. PBI also supports industry oversight and active engagement with the privacy community. PBI believes that strong privacy and information security protections are vital for an effective and trusted data industry.
>
> **11. COMPLIANCE**
>
> PBI will obtain assessments from an independent auditor, who uses procedures and standards generally accepted in the profession to assess PBI's controls relevant to security, availability, and confidentiality, as appropriate.

34. Discovery will show that through their provision of the foregoing services, PBI obtains possession of customers'—including Plaintiffs' and Class Members'—highly sensitive

PII. Thus, in the regular course of their businesses, PBI collects and/or maintains the PII of consumers such as Plaintiffs and Class Members. PBI stores this information digitally in the regular course of business.

35. As evidenced by, *inter alia*, their receipt of the notice informing them that their PII were compromised in the Data Breach, Plaintiffs' and Class Members' PII was transferred using PSC's MOVEit service and/or they otherwise entrusted to Defendants their PII, from which Defendants profited.

36. Yet, contrary to PBI's website representations—by virtue of Defendants' admissions that they experienced the Data Breach—Defendants did not have adequate measures in place to protect and maintain sensitive PII entrusted to them. Instead, Defendants' websites wholly fail to disclose the truth: that Defendants lack sufficient processes to protect the PII that is entrusted to them.

37. In the course of their relationship, clients, including Plaintiff and Class Members, provided Defendants, directly or indirectly, with at least the following PII:

a. names;

b. gender;

c. dates of birth;

d. Social Security numbers; and

e. addresses.

38. In the course of their ordinary business operations, Defendants are entrusted with safeguarding the sensitive PII of Customers.

39. Plaintiffs and Class members are current or former TIAA Customers who provided their Private Information to Defendants.

40. The information held by Defendants at the time of the Data Breach included the

unencrypted Private Information of Plaintiffs and Class members.

41. Upon information and belief, Defendants made promises and representations to Plaintiffs and the Classes that the Private Information collected would be kept safe and confidential, the privacy of that information would be maintained, and Defendants would delete any sensitive information after they were no longer required to maintain it.

42. Indeed, TIAA acknowledges the importance of keeping Private Information safe, stating: "We are committed to your privacy," and "The privacy of your personal information is something we take seriously."[7] Further, TIAA's privacy notice states:

> Security of your information
>
> TIAA protects the personal information you provide against unauthorized access, disclosure, alteration, destruction, loss, or misuse. Your personal information is protected by physical, electronic, and procedural safeguards in accordance with federal and state standards. These safeguards include appropriate procedures for access and use of electronic data, provisions for the secure transmission of sensitive personal information on our website, and telephone system authentication procedures. Additionally, we limit access to your personal information to those TIAA employees and agents who need access in order to offer and provide products or services to you. We also require our service providers to protect your personal information by utilizing the privacy and security safeguards required by law.[8]

43. Plaintiffs and Class members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

44. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class members relied on the sophistication of Defendants to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of

[7] https://www.tiaa.org/public/support/privacy (last visited Aug. 6, 2023).
[8] https://www.tiaa.org/public/support/privacy/privacy-notice (last visited Aug. 6, 2023).

this information. Plaintiffs and Class members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

45. Defendants had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class members from involuntary disclosure to third parties. Defendants have a legal duty to keep Customers' Private Information safe and confidential.

46. Defendants had obligations under the FTC Act, contract, industry standards, and representations made to Plaintiffs and Class members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

47. Defendants derived a substantial economic benefit from collecting Plaintiffs' and Class members' Private Information. Without the required submission of Private Information, Defendants could not perform the services they provide.

48. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class members' Private Information from disclosure.

The Data Breach

49. On or about July 14, 2023, PBI began notifying Customers of the Data Breach, informing them in a Notice:

> On or around May 31, 2021, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

50. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

51. The attacker accessed and acquired files in Defendants' computer systems containing unencrypted Private Information of Plaintiffs and Class members, including their name, Social Security number, date of birth, address, and gender.

52. Plaintiffs' and Class members' Private Information was accessed and stolen in the Data Breach.

53. Plaintiffs further believe their Private Information, and that of Class members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Defendants Acquire, Collect, and Store Plaintiffs' and Class Members' Private Information.

54. As a condition to obtain services from Defendants, Plaintiffs and Class members were required to give their sensitive and confidential Private Information to Defendants.

55. Defendants retain and store this information and derive a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiffs' and Class members' Private Information, Defendants would be unable to perform their services.

56. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

57. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendants to keep their Private

Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

58. Defendants could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class members.

59. Upon information and belief, Defendants made promises to Plaintiffs and Class members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

60. Defendants' negligence in safeguarding the Private Information of Plaintiffs and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendants Knew or Should Have Known of the Risk of a Cyber Attack Because Entities in Possession of Private Information are Particularly Suspectable to Cyber Attacks.

61. Data thieves regularly target entities like Defendants due to the highly sensitive information that they maintain. Defendants knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

62. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities like Defendants that collect and store Private Information and other sensitive information, preceding the date of the Data Breach.

63. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January

2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

64. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiffs and Class members from being compromised.

65. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' server(s), amounting to *millions* of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

66. In its Notice, PBI offers "access to 24 months of complimentary identity monitoring services through Kroll." This is wholly inadequate to compensate Plaintiffs and Class members, as it fails to account for the multiple years of identity theft and financial fraud commonly faced by victims of data breaches and other unauthorized disclosures. It also fails to provide sufficient compensation to Plaintiffs and Class members for the unauthorized release and disclosure of their Private Information. Moreover, once the identity theft service expires, Plaintiffs and Class members will be forced to pay out of pocket for necessary identity monitoring services.

67. The offering of identity theft protection establishes that Plaintiffs' and Class members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendants' computer systems. Moreover, the offer indicates that Defendants recognize that Plaintiffs and Class members are at a present and continuing risk of identity theft and fraud as a result of the Data Breach.

68. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private

Information of Plaintiffs and Class members.

69. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiffs and Class members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

70. Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiffs and Class members and of the foreseeable consequences if their data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class members because of a breach. Nevertheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach.

Defendants Fail to Comply with FTC Guidelines

71. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

72. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[9]

73. The guidelines also recommend that businesses use an intrusion detection system

[9] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Aug. 4, 2023).

to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

74. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

77. Defendants failed to properly implement basic data security practices.

78. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Customers' Private Information or to comply with applicable

[10] *Id.*

industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

79. Upon information and belief, Defendants were at all times fully aware of their obligation to protect the Private Information of the Customers; Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Classes.

Defendants Owed Plaintiffs and Class Members a Duty to Safeguard their Private Information.

80. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the Private Information of Class members.

81. Defendants owed a duty to Plaintiffs and Class members to create and implement reasonable data security practices and procedures to protect the Private Information in their possession, including adequately training their employees and others who accessed Private Information within their computer systems on how to adequately protect Private Information.

82. Defendants owed a duty to Plaintiffs and Class members to implement processes that would detect a compromise of Private Information in a timely manner.

83. Defendants owed a duty to Plaintiffs and Class members to act upon data security

warnings and alerts in a timely fashion.

84. Defendants owed a duty to Plaintiffs and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

85. Defendants owed a duty of care to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate data security practices.

The Data Breach Increases Plaintiffs' and Class Members' Risk of Identity Theft.

86. The unencrypted Private Information of Plaintiffs and Class members will end up (if it has not already ended up) for sale on the dark web, as that is the *modus operandi* of hackers.

87. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class members.

88. Simply put, unauthorized individuals can easily access the Private Information of Plaintiffs and Class members because of the Data Breach.

89. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

90. Plaintiffs' and Class members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class members and to profit from their misfortune.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

91. As a result of the recognized risk of identity theft, when a data breach occurs and

an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

92. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class members must, as Defendants' Notice encourages them to, "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." They must also monitor their financial accounts for many years to mitigate the risk of identity theft.

93. Plaintiffs and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

94. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[11]

95. Plaintiffs' mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports,

[11] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed Aug. 4, 2023).

contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[12]

96. And for those Class members who experience actual identity theft and fraud, the United States Government Accountability Office released the GAO Report, in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

Diminution of Value of Private Information

97. Private Information is valuable property. Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

98. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach—most notably names and Social Security numbers—is difficult, if not impossible, to change.

99. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information… [is] worth more than 10x on the black market."[13]

---

[12] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed Aug. 4, 2023).

[13] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Aug. 4, 2023).

100. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[14]

101. An active and robust legitimate marketplace for Private Information also exists. In fact, the data marketplace is so sophisticated that Customers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[15, 16] Customers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[17]

102. As a result of the Data Breach, Plaintiffs' and Class members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

103. The fraudulent activity resulting from the Data Breach may not come to light for years.

104. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class members are

[14] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[15] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed Aug. 4, 2023).

[16] https://datacoup.com/ (last accessed Aug. 4, 2023).

[17] https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the,software%20installed%20on%20your%20computer (last accessed Aug. 4, 2023).

incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

105. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to millions of individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

106. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class members.

The Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary.

107. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

108. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

109. Consequently, Plaintiffs and Class members are at an increased risk of fraud and

identity theft for many years into the future.

110. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor and protect Class members from the risk of identity theft resulting from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class members would not need to bear, but for Defendants' failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

111. Furthermore, Defendants' poor data security deprived Plaintiffs and Class members of the benefit of their bargain. When agreeing to pay Defendants for the provision of their services, Customers reasonably understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendants did not provide the expected data security. Accordingly, Plaintiffs and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

Plaintiffs' Experiences

Plaintiff Smuda

112. Plaintiff Smuda obtained financial services from TIAAs. To obtain these financial services, she was required to provide her Private Information to Defendants.

113. Upon information and belief, at the time of the Data Breach— on May 29 and May 30, 2023—Defendants retained Plaintiff Smuda's Private Information in their system.

114. Plaintiff Smuda is very careful about sharing her sensitive Private Information. Plaintiff Smuda stores any documents containing her Private Information in a safe and secure location. Plaintiff Smuda has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

115. Plaintiff Smuda received a Notice from PBI on or about July 14, 2023. According to the Notice, Plaintiff Smuda's Private Information was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, date of birth, address, and gender.

116. As a result of the Data Breach, Plaintiff Smuda made reasonable efforts to mitigate the impact of the Data Breach, including checking her bills and accounts to make sure they were correct. Plaintiff Smuda has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

117. As a result of the Data Breach, Plaintiff Smuda fears for her personal financial security and uncertainty over what Private Information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

118. As a result of the Data Breach, Plaintiff Smuda anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

119. As a result of the Data Breach, Plaintiff Smuda is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

120. Plaintiff Smuda has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Checchia

121. Plaintiff Checchia obtained financial services from TIAA. To obtain these financial

services, he was required to provide his Private Information to Defendants.

122. Upon information and belief, at the time of the Data Breach— on May 29 and May 30, 2023—Defendants retained Plaintiff Checchia's Private Information in their system.

123. Plaintiff Checchia is very careful about sharing his sensitive Private Information. Plaintiff Checchia stores any documents containing his Private Information in a safe and secure location. Plaintiff Checchia has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

124. Plaintiff Checchia received a Notice from PBI on or about July 14, 2023. According to the Notice, Plaintiff Checchia's Private Information was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, date of birth, address, and gender.

125. As a result of the Data Breach, Plaintiff Checchia made reasonable efforts to mitigate the impact of the Data Breach, including checking his bills and accounts to make sure they were correct. Plaintiff Checchia has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

126. As a result of the Data Breach, Plaintiff Checchia paid Aura, a security company, $114.48 for credit monitoring services.

127. As a result of the Data Breach, Plaintiff Checchia fears for his personal financial security and uncertainty over what Private Information was revealed in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

128. As a result of the Data Breach, Plaintiff Checchia anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

129. As a result of the Data Breach, Plaintiff Checchia is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

130. Plaintiff Checchia has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

131. Pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiffs bring this action on behalf of themselves and the following classes:

(1) PSC Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach.

(a) PSC Illinois Class: All residents of Illinois whose Private Information was compromised in the MOVEit data breach.

(b) PSC Pennsylvania Class: All residents of Pennsylvania whose Private Information was compromised in the MOVEit data breach.

The foregoing state-specific PSC classes are collectively referred to as the "PSC State Classes."

(2) PBI Nationwide Class: All persons whose Private Information was compromised on PBI's platform and/or systems in the MOVEit data breach.

(a) PBI Illinois Class: All residents of Illinois whose Private Information was compromised on PBI's platform and/or systems in the MOVEit data breach.

(b) PBI Pennsylvania Class: All residents of Pennsylvania whose Private Information was compromised on PBI's platform and/or systems in the MOVEit data breach.

The foregoing state-specific PBI classes are collectively referred to as the "PBI State Classes."

(3) TIAA Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by TIAA.

(a) TIAA Illinois Class: All residents of Illinois whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by TIAA.

(b) TIAA Pennsylvania Class: All residents of Pennsylvania whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by TIAA.

The foregoing state-specific TIAA classes are collectively referred to as the "TIAA State Classes."

132. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

133. Plaintiffs reserve the right to amend the definition of the Classes or add a class or sub-class if further information and discovery indicate that the definition of the Classes should be narrowed, expanded, or otherwise modified.

134. **Numerosity**: The Class members are so numerous that joinder of all members is impracticable, if not completely impossible. Over 2.5 million individuals were affected by the Data Breach. The Class members are apparently identifiable within Defendants' records, and Defendants have notified these individuals. *See, e.g.*, Notice.

135. Common questions of law and fact exist as to all Class members and predominate over any questions affecting solely individual Class members. Among the questions of law and fact common to the Classes that predominate over questions which may affect individual Class members, are the following:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiffs and Class members;

b. Whether Defendants had respective duties not to disclose the Private Information of Plaintiffs and Class members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the Private Information of Plaintiffs and Class members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiffs and Class members;

e. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Plaintiffs and Class members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct; and

h. Whether Plaintiffs and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

136. **Typicality:** Plaintiffs' claims are typical of those of the other Class members because Plaintiffs, like every other Class member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Classes.

137. This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendants'

policies challenged herein apply to and affect Class members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

138. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of Class members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class members. Plaintiffs seek no relief that is antagonistic or adverse to Class members and the infringement of the rights and the damages they have suffered are typical of other Class members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

139. **Superiority**: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that millions of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

140. The nature of this action and the nature of laws available to Plaintiffs and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources;

the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

141. Adequate notice can be given to Class members directly using information maintained in Defendants' records.

142. Further, Defendants have acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

a. Whether Defendants owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendants' failure to institute adequate protective security measures amounted to breach of an implied contract;

e. Whether Defendants was unjustly enriched by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Private Information.

f. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and

g. Whether adherence to FTC data security recommendations and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence

143. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

144. All Plaintiffs bring this claim against PSC, PBI, and TIAA on behalf of the PSC, PBI, and TIAA Nationwide Classes or, in the alternative, the PSC State Classes, PBI State Classes, and the TIAA State Classes.

145. Defendants require Customers, including Plaintiffs and Class members, to submit non-public Private Information in the ordinary course of providing financial services.

146. Defendants gathered and stored the Private Information of Plaintiffs and Class members as part of their business of soliciting Customers, which solicitations and services affect commerce.

147. Plaintiffs and Class members entrusted Defendants with their Private Information with the understanding that Defendants would safeguard their information.

148. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class members could and would suffer if the Private Information were wrongfully disclosed.

149. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class members' Private Information

held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

150. Defendants owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

151. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and the Customers. That special relationship arose because Plaintiffs and Class members entrusted Defendants with their confidential Private Information, a necessary part of being Customers of Defendants.

152. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants is bound by industry standards to protect confidential Private Information.

153. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

154. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, (a) failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information; (b) failing to adequately monitor the security of their networks and systems; and (c) allowing unauthorized access to Class members' Private Information.

155. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the

Class was reasonably foreseeable, particularly considering Defendants' inadequate security practices.

156. It was foreseeable that Defendants' failure to use reasonable measures to protect Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

157. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class members could and would suffer if the Private Information were wrongfully disclosed.

158. Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and Class members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems.

159. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

160. Plaintiffs and Class members had no ability to protect their Private Information that was in, and likely remains in, Defendants' possession.

161. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

162. Defendants' duty extended to protecting Plaintiffs and Class members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

163. Defendants have admitted that the Private Information of Plaintiffs and Class members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

164. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and Class members, the Private Information of Plaintiffs and Class members would not have been compromised.

165. There is a close causal connection between Defendants' failure to implement security measures to protect the Private Information of Plaintiffs and Class members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class members. The Private Information of Plaintiffs and Class members was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

166. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

167. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class

members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

168. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

169. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

170. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT II
Negligence *Per Se*

171. Plaintiffs re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

172. All Plaintiffs bring this claim against PSC, PBI, and TIAA on behalf of the PSC, PBI, and TIAA Nationwide Classes or, in the alternative, the PSC State Classes, PBI State Classes, and the TIAA State Classes.

173. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

174. Defendants breached their duties to Plaintiffs and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

175. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se.*

176. The injuries to Plaintiffs and Class members resulting from the Data Breach were directly and indirectly caused by Defendants' violation of the statute described herein.

177. Plaintiffs and Class members were within the class of persons the FTC Act were intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statue was intended to guard against.

178. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

179. The injuries and harms suffered by Plaintiffs and Class members were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that Defendants' breach would cause Plaintiffs and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

180. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class members have suffered injuries and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract

181. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in in the preceding paragraphs.

182. All Plaintiffs bring this claim against PSC, PBI, and TIAA on behalf of the PSC, PBI, and TIAA Nationwide Classes or, in the alternative, the PSC State Classes, PBI State Classes, and the TIAA State Classes.

183. Defendants offered to provide financial services to the Customers, including Plaintiffs and Class members, in exchange for payment.

184. Defendants also required Plaintiffs and Class members to provide Defendants with their Private Information to receive services from Defendants.

185. In turn, Defendants impliedly promised to protect Plaintiffs' and Class members' Private Information through adequate data security measures.

186. Customers accepted Defendants' offer by providing Private Information to Defendants in exchange for receiving Defendants' services, and then by paying for and receiving the same.

187. Plaintiffs and Class members would not have entrusted their Private Information to Defendants but-for the above-described agreement with Defendants.

188. Defendants materially breached their agreement(s) with Plaintiffs and Class members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

189. Plaintiffs and Class members have performed under the relevant agreements, or such performance was waived by the conduct of Defendants.

190. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the

parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

191. Defendants' conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

192. The losses and damages Plaintiffs and Class members sustained as described herein were the direct and proximate result of Defendants' breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

COUNT IV
Unjust Enrichment
(On behalf of Plaintiffs and all Class members)

193. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in in the preceding paragraphs.

194. All Plaintiffs bring this claim against PSC, PBI, and TIAA on behalf of the PSC, PBI, and TIAA Nationwide Classes or, in the alternative, the PSC State Classes, PBI State Classes, and the TIAA State Classes.

195. This Count is brought in the alternative to Count III, Breach of Implied Contract.

196. Plaintiffs and Class members conferred a monetary benefit on Defendants by providing Defendants with their valuable Private Information. In doing so, Plaintiffs and Class members understood that part of the benefit Defendants derived from the Private Information would be applied to data security efforts to safeguard the Private Information.

197. Defendants enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Private Information.

198. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and

Class members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

199. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

200. Defendants acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

201. If Plaintiffs and Class members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants.

202. Plaintiffs and Class members have no adequate remedy at law.

203. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Private Information in their continued possession and (vii) future costs in terms of time, effort, and money that will be

expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

204. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

205. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them.

COUNT V
Declaratory Judgment

206. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs.

207. All Plaintiffs bring this claim against PSC, PBI, and TIAA on behalf of the PSC, PBI, and TIAA Nationwide Classes or, in the alternative, the PSC State Classes, PBI State Classes, and the TIAA State Classes.

208. Defendants owes duties of care to Plaintiffs and Class members that require Defendants to adequately secure their Private Information.

209. Defendants still possess Plaintiffs' and Class members' Private Information.

210. Plaintiffs and Class members are at risk of harm due to the exposure of their Private Information and Defendants' failure to address the security failings that lead to such exposure.

211. Plaintiffs, therefore, seek a declaration that (1) Defendants' existing security measures do not comply with their duties of care to provide reasonable security procedure and practices appropriate to the nature of the information to protect Customers' Private Information, and (2) to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal

security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

Purchasing credit monitoring services for Plaintiffs and Class members for a period of ten years; and

g. Meaningfully educating Plaintiffs and Class members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class members, requests judgment against Defendants and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and

their Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

requiring Defendants to delete, destroy, and purge the Private Information of Plaintiffs and Class members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class members;

iii. requiring Defendants to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class members;

iv. prohibiting Defendants from maintaining the Private Information of Plaintiffs and Class members on a cloud-based database;

v. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct

testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

viii. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and security checks;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. requiring Defendants to implement logging and monitoring programs

sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct an attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined by a jury at trial;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: June 12, 2024

Respectfully Submitted,

/s/ Kristen A. Johnson

Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

Andrew J. Shamis
SHAMIS & GENTILE P.A.
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Tel: (305) 479-2299
ashamis@shamisgentile.com

Jeff Ostrow*
Kristen Lake Cardoso*
Steven Sukert
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500 Fort
Lauderdale, Florida 33301
Tel: (954) 525-4100
ostrow@kolawyers.com
cardoso@kolawyers.com
sukert@kolawyers.com

MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC
Gary Klinger*
227 West Monroe Street, Suite 2100
Chicago, Illinois 60606
Tel: (866) 252-0878
GKlinger@milberg.com

Attorneys for Plaintiffs and the Putative Classes

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL
PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Plaintiffs' Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was served by filing it on the Court's CM/ECF system, which will automatically send a notification of such filing to all counsel of record via electronic mail.

Dated: June 12, 2024

/s/ Kristen Johnson
Kristen Johnson